EXHIBIT 3

SheppardMullin

Sheppard, Mullin, Richter & Hampton LLP
Four Embarcadero Center, 17th Floor
San Francisco, California 94111-4109
415.434.9100 main
415.434.3947 fax
www.sheppardmullin.com

Lai L. Yip
415.774.3147 direct
lyip@sheppardmullin.com

File Number: 02HL-350124

April 13, 2022

VIA E-MAIL ONLY

Rory S. Miller, Esq. Rory.Miller@LockeLord.Com
Mitchell J. Popham, Esq. mpopham@lockelord.com
William Mullen, Esq. william.mullen@lockelord.com
Joseph N. Froelich, Esq. jfroehlich@lockelord.com
LOCKE LORD LLP
300 S. Grand Avenue, Suite 2600
Los Angeles, California 90071

Josh Krevitt, Esq. jkrevitt@gibsondunn.com
Kate Dominguez, Esq. kdominguez@gibsondunn.com
Ilissa Samplin, Esq. isamplin@gibsondunn.com
Angelique Kaounis, Esq. akaounis@gibsondunn.com
Michael M. Polka, Esq. mpolka@gibsondunn.com
Justine Goeke, Esq. jgoeke@gibsondunn.com
GIBSON, DUNN, & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193

Re: Inspection Protocol in *Moog Inc. v. Skyryse, Inc., et al.*, W.D.N.Y., No. 1:22-cv-00187

Dear Counsel:

We write to address the protocol regarding inspection of discovery materials to be hosted by iDS ("Inspection Materials"), and particularly the insufficiency of Defendants' proposed protocol. The most fundamental deficiencies of Defendants' proposed protocol are that it does not permit a party's Experts or Outside Counsel to directly inspect the Inspection Materials and limits the scope of inspection to searching of file names and hash values. For reasons explained below, this framework would effectively erect a wall between Moog and the Inspection Materials and hobble Moog's investigation into Defendants' misappropriation. This is highly improper and unacceptable in this case.

I. Permitting Experts and Outside Counsel to Directly Inspect Is Proper and Any Privilege Concerns Can Be Readily Addressed

As a general matter, and contrary to the assertions in your April 8, 2022 email, it is common for a defendant in a trade secret case to permit a plaintiff's outside counsel and retained experts to directly inspect the Defendants' highly confidential information. Such access here to Experts and

Outside Counsel is not "unfettered," as you say, because the access is subject to the protections of the protective order that will be entered in this case. Moreover, the privilege concerns you raised can be adequately addressed through a presumptive privilege filter—e.g., a filter whereby iDS would use keywords to cull out presumptively privileged documents from the forensic image of the devices, while the remainder is made available for inspection to Moog's Experts and Outside Counsel. (We note that such a filter would not need to be applied to information iDS collects *about* the devices, such as photographs of the devices and information about the specifications and serial number identifiers of those devices.) For example, the filter can cull out materials based on names of all defense counsel (external and internal), the names of their respective law firms, etc. Defendants would then have a set amount of time (e.g., two weeks) to review the presumptively privileged documents and determine whether they are in fact privileged (or whether they are not and therefore need to be made available for inspection). In the meantime, Moog's Outside Counsel and Experts can inspect the remaining materials not culled out by the presumptive privilege filter. Applying presumptive privilege filters is common in litigation involving very high volumes of discovery materials. If anything is not caught by the presumptive privilege filter, and authorized reviewers (i.e., Outside Counsel and Experts) come across privileged documents, they will promptly notify Defendants so that such documents may be clawed back pursuant to F.R.C.P. 26(b)(5)(B) or other procedures that the parties may agree to.

II. Permitting Experts and Outside Counsel to Directly Inspect Is Necessary in This Case Specifically

Beyond being common in litigation, permitting Experts and Outside Counsel to directly inspect the Inspection Materials is absolutely necessary here—and is the only approach that will facilitate Moog's effective prosecution of this case and the effective identification of the full scope of misappropriation (especially given Defendants' unwillingness and claimed inability to fully comply with the stipulated TRO). The insufficiency of Defendants' proposed approach—i.e., limiting inspection access to only iDS and limiting search parameters to just file names and hash values—is readily demonstrated by examination of how such limitations would adversely impact the inspection of three categories of Inspection Materials, as explained below: (1) source code and other technical documents; (2) process assets; and (3) forensic data regarding devices.[1]

A. *Source Code and Other Technical Documents*

1. Limiting inspection to search of file names and hash values is insufficient.

Defendants have collectively stolen at least about 1.5 million documents, a significant amount of which was source code and other technical documents, from projects such as eRTOS, Platform, and so forth. We expect that the wholesale further copying of these files, unaltered, by Skyryse employees onto Skyryse's network or other Skyryse devices to be just a slim minority of Skyryse's misappropriating use of these files, for at least several reasons. One is that a significant number of these files contain Moog proprietary statements, e.g., statements with headers like "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION." We would not expect Skyryse employees to wholesale copy a file, unaltered, because the inclusion of the

[1] To be clear, these three categories are provided as examples only and are not limiting.

Moog proprietary statement would make the theft too obvious. Another reason is that a whole file (as opposed to just portions of a file) may be more difficult to "plug" into the existing Skyryse projects or systems.

Instead, we expect the vast majority of Skyryse's misappropriation to involve Skyryse employees treating source code and other technical documents as more of a "reference library" as they are developing Skyryse processes and products. For example, Skyryse employees are likely to pick and choose portions from the Moog "reference library" (e.g., a function here, a function there) to copy or incorporate into Skyryse documents, carefully excluding portions with the term "Moog" in them such as the Moog proprietary statement, and replacing names and terms distinctive to Moog in order to obfuscate the theft. Skyryse employees are also likely to use Moog files as a visual reference while they draft Skyryse documents—for example, using the same algorithms, structures, process flows, etc., but using different words to implement the foregoing (in order to, among other things, obfuscate the theft).

Searching for exact file names and hash values is useless to identify the kinds of misappropriation identified above. This is because such searching would, at best, uncover wholesale copying of entire files where neither the file names nor even a single character of the files are altered. Indeed, the inadequacy of searching for file names and hash values has been demonstrated and proven during the TRO process—Defendants have employed this very technique and failed to adequately identify the stolen materials and comply with the TRO.

2. Moog's Retained Expert Can Conduct the Inspection Necessary, Not iDS

As explained above, the misappropriating use of source code and other technical documents that is at the heart of this case and described above cannot be adequately identified using merely file names or hash values (as Defendants have proposed) or other search terms. These mechanical, superficial, brute force methods will not work. Instead, conducting an adequate inspection requires a more sophisticated, nuanced approach, executed by someone with both deep expertise in software development as well as knowledge and familiarity with software development specifically in the aviation context. For example, the Expert must analyze how Skyryse's flight control software is architected and the extent and nature of that architecture's similarities to Moog's, including by visually comparing code side-by-side where necessary. As another example, the Expert must know what the relevant source code looks like, analyze Skyryrse's repository logs to identify large check-ins of such source code, and exercise judgment based on experience to determine whether such check-ins are unusual and atypical in aviation software development.

iDS does not have the above expertise, and we never proposed or agreed to iDS with the intent that they would serve in the role of reviewer and inspector of materials. Indeed, none of the parties raised these capabilities with iDS during the vetting process and communications with iDS prior to engaging iDS on April 1. The March 11 Stipulated TRO expressly leaves the details of who will conduct the inspection and how the inspection will be conducted unaddressed, instead stating generally that the parties shall "agree on a protocol for searching all such information delivered to the Forensics Firm." It does *not* say, for example, that the parties shall "agree on a protocol for searching ***by the Forensic Firm of*** all such information delivered to the

Forensics Firm." And certainly, it was never our intent that the Forensic Firm do so. Instead, our intent was that iDS host the data securely, so that neither party takes possession of the Inspection Materials in the first instance, and make proper forensic images of the data for the parties' inspection. Nor does the stipulation say that the parties shall "agree on a protocol for searching ***for file names and hash values in*** all such information delivered to the Forensics Firm." The foregoing said, if *Defendants* want to solely use iDS to search materials using file names and hash values for the purpose of their defense, that is Defendants' choice. But Moog will not be deprived of its choice of expert or reasonable methods of inspection to adequately prosecute its case.

Further to this point, we note that on the parties' meet and confer last Thursday, Defendants repeatedly suggested *they* lacked the capability and understanding to conduct the necessary inspection in this case, asking repeatedly for *Moog* to identify what they could search for besides file names and hash values. iDS is far further removed from this case than the Defendants are, further confirming that iDS cannot undertake such an inspection on a substantive basis.

B. *Process Assets*

The insufficiency of Defendants' proposed protocol is also demonstrated by examination of another category of Inspection Materials, i.e., process assets.

In addition to source code and related technical documents, Defendants also stole Moog's repository of process assets, e.g., templates, checklists, tools, test cases, artifacts,[2] etc. pertaining to DO-178 compliance certification. As Defendants know, the development of flight software hinges on compliance with DO-178, a government standard that a company must follow in order to develop software for use in FAA airspace. Moog has spent years developing the process assets to ensure compliance with DO-178. This includes a large template library, for example, that sets the framework for software development that is compliant with DO-178 and FAA safety requirements, and which would be used in the compliance approval and certification process. In fact, because Moog develops software at the highest level of criticality, much more time is spent on testing, reviews, and development of documentation that support the artifacts to show that the code complies with DO-178, than on the code itself. These process assets take years to develop.

We believe Skyryse is particularly interested in these extremely valuable process assets because it is seeking DO-178 compliance certification, but did not (prior to the theft and poaching of employees) have background or experience in this area. For example, while at Moog, Mr. Pilkington developed a Python-based qualification tool for automated verification called MDTE (Moog Desk Top Environment), which follows the DO-330 standard. This tool is used to test flight software in connection with DO-178 compliance certification. This tool is valuable because it automates the verification process (which, as explained above, constitutes the majority of time spent by Moog on software development) and therefore saves time and money. By stealing this

[2] An "artifact" as used here is a completed checklist that proves the company has reviewed the source code at issue and that the code is correct, which would be presented to the FAA in the case of an audit.

tool and either referencing the tool or copying portions of it, Skyryse is able to fast-track what would otherwise take years to develop, especially given its own (prior) lack of background and experience in compliance certification. By developing a software process using Moog's library of artifacts and other process assets, Skyryse can do in an 8-hour day what would otherwise have taken years of effort.

1. Limiting inspection to search of file names and hash values is insufficient.

Similar to source code and technical documents, Moog's process assets are less likely to be copied wholesale by Skyryse employees into Skyryse systems and devices, and more likely to be used as a Moog "reference library." This is true not only because there are markers specific to Moog in these process assets (making theft too obvious from wholesale copying), but because these process assets need to be adapted to Skyryse's existing projects and systems. Skyryse employees are most likely to pick and choose what they like from these process assets, changing distinctive terms and names and otherwise obfuscating the theft as they go along.

Searching for hash values and file names are largely useless to identify such misappropriation.

2. Moog's Retained Expert Can Conduct the Inspection Necessary, Not iDS

To identify misappropriation of process assets involves analyzing Skyryse's process assets to determine whether they were developed by reference to and misappropriation of Moog's process assets. For example, the Expert must analyze Skyryse's process for generating artifacts and whether it mimics Moog's artifacts; and compare the parties' templates, checklists, and other process assets for telltale similarities. DO-178, the governing compliance standard, is very unique and particular, with prescriptive requirements for how a company develops aviation software in order to be in compliance. The Expert needs to have knowledge of DO-178 and related compliance testing and certification procedures in order to adequately analyze the process assets. To determine whether similarities between DO-178 process assets are unusual and likely the result of copying (rather than what you might typically find in process assets) requires the right experience and the execution of informed judgment. This is not a mechanical exercise, but instead requires someone with the right expertise in aviation software development.

iDS does not have the expertise to conduct the inspection described above. iDS does not have experts in aviation software development, DO-178, and related compliance procedures and certification. Nor should it, because that is not a set of qualifications that iDS was screened for; and it is outside the scope of the work iDS was retained to perform. We would note that even in a more "ordinary" case of software theft—without all the process assets described above that are so specific to government regulations in the aviation industry—parties routinely rely on experts with specific source code and industry experience to conduct reviews and inspections. Here, iDS cannot fulfill the role necessary in order to uncover the misappropriation at the heart of this case.

C. *Forensic Data Regarding Devices*

In order for Moog to determine the scope of Defendants' misappropriation, its Expert must be able to conduct a forensic inspection of at least the 23 devices Defendants have turned over to iDS—e.g., review forensic images of the 23 devices, along with photographs of the devices and information about the specifications and serial number identifiers of those devices. Such a forensic inspection will facilitate the determination of when and how those devices were accessed, and whether data from those devices were transferred to other devices (including ones we may not currently know about) or onto the Skyryse network. For example, the Expert needs to determine through such a forensic inspection of the 23 devices at least: (1) whether and when folders containing stolen Moog data were accessed, and from what other devices; (2) whether and when stolen Moog files were viewed or edited, and from what other devices; (3) when and what Moog data was transferred from any of the 23 devices and to where, and vice versa; and (4) when and what Moog data ultimately migrated to Skyryse's network through any of these 23 devices. The Expert needs access to forensic data reflecting device history like date and time stamps pertaining to connections to other devices, file access histories, file download histories, file upload histories, and so forth—in sum, the Expert needs to determine what Defendants have been doing with Moog's data since at least November 2021.

A search for just file names and hash values clearly would not satisfy the above objectives. Nor would it make sense for iDS to conduct the above forensic inspection itself, rather than Moog's own Expert. That would only inject needless and unacceptable delay into the discovery schedule, with far less effective results. It would make no sense for Moog's Expert, for example, to provide instructions to iDS on what steps to take, have iDS take a week to execute on those steps against 23 devices and send back the results, have Moog's Expert review those results and tell iDS the next set of steps based on that review, have iDS take another week to execute on the new set of steps against the 23 devices, and so forth iteratively ad infinitum. That is completely inefficient and would take too long and result in a massive and unnecessary prolongation of the expedited discovery schedule. Moog's Expert knows the case, knows what to look for, and needs to be able to conduct the inspection himself, following leads as he finds them and adjusting his direction and process as he goes along. Moreover, because the parties' communications with iDS should not be *ex parte*, Moog's Expert's instructions to iDS (i.e., his work product) would become known to Defendants, which is unacceptable, not only because Defendants are not entitled to this work product but because Defendants should invest their own resources into their own expert.

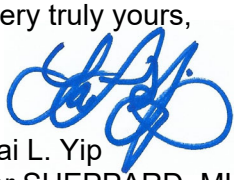
III. Conclusion

Defendants' proposed protocol—which permits only the superficial searching of file names and hash values by a neutral vendor—appears deliberately designed to hobble Moog's ability to identify the egregious theft and misappropriating use that Defendants have engaged in. Defendants are in possession of (or have deliberately spoliated) nearly all the evidence of theft and misappropriation in this case, and know exactly what they took and what they have done with it—yet appear to be attempting to erect a wall between Moog and that evidence. That is extremely concerning and, to us, very strong confirmation that egregious misappropriation has indeed occurred and that Defendants seek to hide it from Moog and the Court.

SheppardMullin

We request that Defendants withdraw their proposed protocol and agree to the protocol that Moog proposed. If Defendants decline to do so, please let us know when you are available to meet and confer about these issues Thursday or Friday of this week.

Very truly yours,



Lai L. Yip
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

SMRH:4863-8531-2027

cc: Rena Andoh, Esq.
Travis Anderson, Esq.
Kazim A. Naqvi, Esq.
Robert J. Fluskey, Jr., Esq.
Melissa N. Subjeck, Esq., Esq.